JUST
Jordan University of Science & Technology

Faculty of Engineering

Department of Electrical Engineering

Undergraduate project

Dual Band Mobile Jammer for GSM 900 & GSM 1800

Done by:

Ahmed Sudqi Hussein Abdul-Rahman

Ahmad Nasr Raja Mohammad

Supervised by:

Prof. Nihad Dib

Table of contents

Abstract

This report presents the design, implementation, and testing of a dual-band cell-phone jammer. This jammer works at GSM 900 and GSM 1800 simultaneously and thus jams the three well-known carriers in Jordan (Zain, Orange, and Umniah). This project went through two phases:

Phase one: studying the GSM-system to find the best jamming technique, establishing the system design and selecting suitable components.

Phase two: buying all the needed components, drawing the overall schematics, fabricating the PCB layout, assembling the devices, performing some measurements and finally testing the mobile jammer.

The designed jammer was successful in jamming the three carriers in Jordan as will be shown at the end of this report.

1. Introduction

Communication jamming devices were first developed and used by military. This interest comes from the fundamental objective of denying the successful transport of information from the sender (tactical commanders) to the receiver (the army personnel), and vice-versa. Nowadays, mobile (or cell) phones are becoming essential tools in our daily life. Here in Jordan, for example, with a rather low population (around 5 million), three main cell phone carries are available; namely; Zain, Orange, and Umniah The first two use the GSM 900 system, while the third uses the GSM 1800 system. Needless to say, the wide use of mobile phones could create some problems as the sound of ringing becomes annoying or disrupting. This could happen in some places like conference rooms, law courts, libraries, lecture rooms and mosques. One way to stop these disrupting ringings is to install a device in such places which will inhibit the use of mobiles, i.e., make them obsolete. Such a device is known as cell phone jammer or "GSM jammer", which is basically some kind of electronic countermeasure device. The technology behind cell phone jamming is very simple. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen. All phones within the effective radius of the jammer are silenced. It should be mentioned that cell phone jammers are illegal devices in most countries. According to the Federal Communications Commission (FCC) in the USA: "The manufacture, importation, sale, or offer for sale, of devices designed to block or jam wireless transmissions is prohibited". However, recently, there has been an increasing demand for portable cell phone jammers. We should mention that this project, presented in this report, is solely done for educational purposes. There is no intention to manufacture or sell such devices in Jordan, or elsewhere. In this project, a device that will jam both GSM 900 and GSM 1800 services will be designed, built, and tested.

2. Jamming Techniques

There are several ways to jam an RF device. The three most common techniques can be categorized as follows:

1. Spoofing

In this kind of jamming, the device forces the mobile to turn off itself. This type is very difficult to be implemented since the jamming device first detects any mobile phone in a specific area, then the device sends the signal to disable the mobile phone. Some types of this technique can detect if a nearby mobile phone is there and sends a message to tell the user to switch the phone to the silent mode (Intelligent Beacon Disablers).

2. Shielding Attacks

This is known as TEMPEST or EMF shielding. This kind requires closing an area in a faraday cage so that any device inside this cage can not transmit or receive RF signal from outside of the cage. This area can be as large as buildings, for example.

3. Denial of Service

This technique is referred to DOS. In this technique, the device transmits a noise signal at the same operating frequency of the mobile phone in order to decrease the signal-to-noise ratio (SNR) of the mobile under its minimum value. This kind of jamming technique is the simplest one since the device is always on. Our device is of this type.

3. Design Parameters

Based on the above, our device which is related to the DOS technique is transmitting noise on the same frequencies of the two bands GSM 900 MHz, and GSM 1.8 GHz (known also as DCS 1800 band). We focused on some design parameters to establish the device specifications. These parameters are as follows:

1. The distance to be jammed (D)

This parameter is very important in our design, since the amount of the output power of the jammer depends on the area that we need to jam. Later on we will see the relationship between the output power and the distance D. Our design is established upon D=10 meters for DCS 1800 band and D=20 meters for GSM 900 band.

2. The frequency bands

Table 1: Operating frequency bands.

	UPLINK (Handset transmit)	**DOWNLINK** (Handset receive)	**USED IN JORDAN BY:**
GSM 900	890-915 MHz	935-960 MHz	Zain + Orange
DCS 1800	1710-1785 MHz	1805-1880 MHz	Umniah

In our design, the jamming frequency must be the same as the downlink, because it needs lower power to do jamming than the uplink range and there is no need to jam the base station itself. So, our frequency design will be as follows:

GSM 900 ⟶ 935-960 MHz
GSM 1800 ⟶ 1805-1880 MHz

3. Jamming–to-signal ratio {J/S}

Jamming is successful when the jamming signal denies the usability of the communication transmission. In digital communications, the usability is denied when the error rate of the transmission can not be compensated by error correction. Usually, a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver (mobile device).

The general equation of the jamming-to-signal ratio is given as follows:

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j}$$

where: P_j=jammer power, G_{jr}= antenna gain from jammer to receiver, G_{rj}=antenna gain from receiver to jammer, R_{tr}=range between communication transmitter and receiver, B_r=communication receiver bandwidth, L_r =communication signal loss, P_t=transmitter power, G_{tr}= antenna gain from transmitter to receiver, G_{rt}=antenna gain from receiver to transmitter, R_{jr}=range between jammer and communication receiver, B_j=jammer bandwidth, and L_j=jamming signal loss.

For GSM, the specified system SNR_{min} is 9 dB which will be used as the worst case scenario for the jammer. The maximum power at the mobile device P_r is -15 dBm.

4. Free space loss {F}

The free-space loss (or path loss) is given by:

$$\text{Path loss (dB)} = 32.44 + 20 \log d\,(\text{km}) + 20 \log f\,(\text{MHz})$$

The maximum free space loss (worst case F) happens when the maximum frequency is used in the above equation. Using 1880 MHz gives:

F (dB) =32.44+20 log 0.01 + 20 log 1880 which gives F =58 dB.

4. System Design

4.1 Power calculations

Here, we need to find the power that is needed to be transmitted to jam any cell phone within a distance of around 10 meters for DCS. From the above considerations, we can find the required output power from the device, as follows:

Using SNR=9 dB and the maximum power signal for mobile receiver=-15 dBm, gives J=-24 dBm. But, our goal is to find the output power from the device, so when we add the free space loss to the amount of power at the mobile receiver we get our target:

Output power=-24dBm+58dB = 34 dBm

4.2 Parts of the jammer device

Figure 1 shows the block diagram for the jammer to be designed.

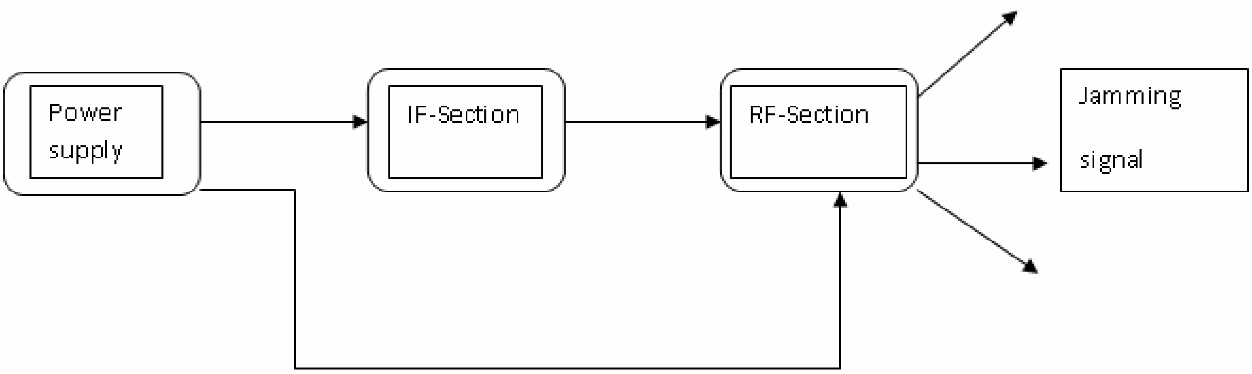


Figure 1 Jammer main blocks.

4.2.1 The Power supply

This is used to supply the other sections with the needed voltages. Any power supply consists of the following main parts:

Transformer: - is used to transform the 220VAC to other levels of voltages.

Rectification: - this part is to convert the AC voltage to a DC one. We have two methods for rectification:

A] Half wave-rectification: the output voltage appears only during positive cycles of the input signal.

B] Full wave –rectification: a rectified output voltage occurs during both the positive and negative cycles of the input signal.

The Filter: used to eliminate the fluctuations in the output of the full wave rectifier "eliminate the noise" so that a constant DC voltage is produced. This filter is just a large capacitor used to minimize the ripple in the output.

Regulator: this is used to provide a desired DC-voltage.

Figure 2 shows the general parts of the power supply.

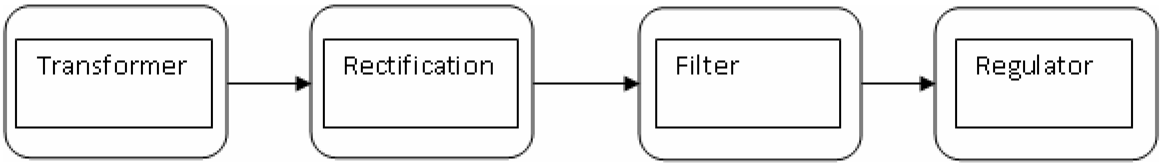


Figure 2 Parts of the power supply.

In our project we need 12, -12, 5 and 3.5 volts. We found that the PC power supply can provide all the voltages that we need in the jammer, so we bought one.

4.2.2 The IF-section

The tuning section of the jammer sweeps the VCO through the desired range of frequencies. Basically, it is just a triangle or sawtooth-wave generator; offset at a proper amount so as to sweep the VCO from the minimum desired frequency to a maximum. The tuning signal is generated by a triangular wave mixed with noise. The IF section consists of three main parts:

1. Triangle wave generator. (To tune the VCO in the RF section)
2. Noise generator (provides the output noise).
3. Mixer" summer" (to mix the triangle and the noise waves).

Triangle wave generator:

The main use of the triangle wave is to sweep the VCO through the desired frequency range. We want to cover the downlink through our VCO, i.e., 935-960 MHz for VCO66CL, and 1805-1880MHz for VCO55BE.

In our design, we will use 555timer IC operating in the a-stable mode to generate the sweeping signal. The output frequency depends on the charging and discharging of the capacitor, resistors values and the power supply for the IC. Figure 3 shows how we can use the 555timer in the general A-stable mode

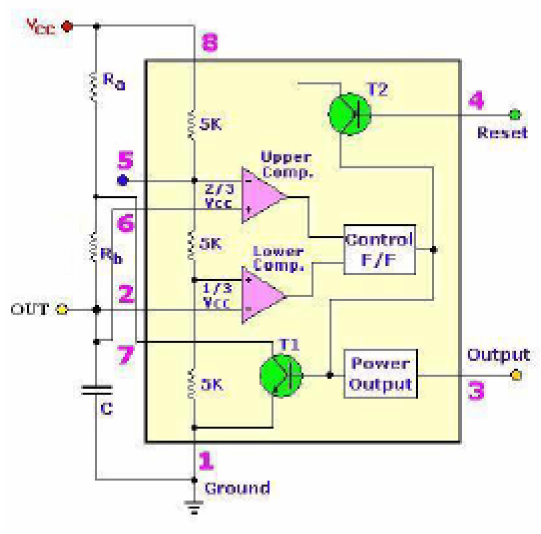


Figure 3 A-stable 555timer.

The charging time for the capacitor can be found as follows:

$$T_c = .693(R_a + R_b)C$$

For discharging time, the following equation can be used:

$$T_D = .693R_bC$$

The output frequency can be calculated as follows:

$$f = \frac{1.44}{(Ra + 2Rb)C}$$

In our project, we need to get the duty cycle (D.C.) equal to 50% which means the time needed for charging equals the discharging time. This can be done by using Ra=Rb and placing a diode across Rb. The following equation shows the output frequency:

$$f = \frac{1.44}{(Ra + Rb)C}$$

Figure 4 shows the connection for the A-stable mode with D.C.=50%.

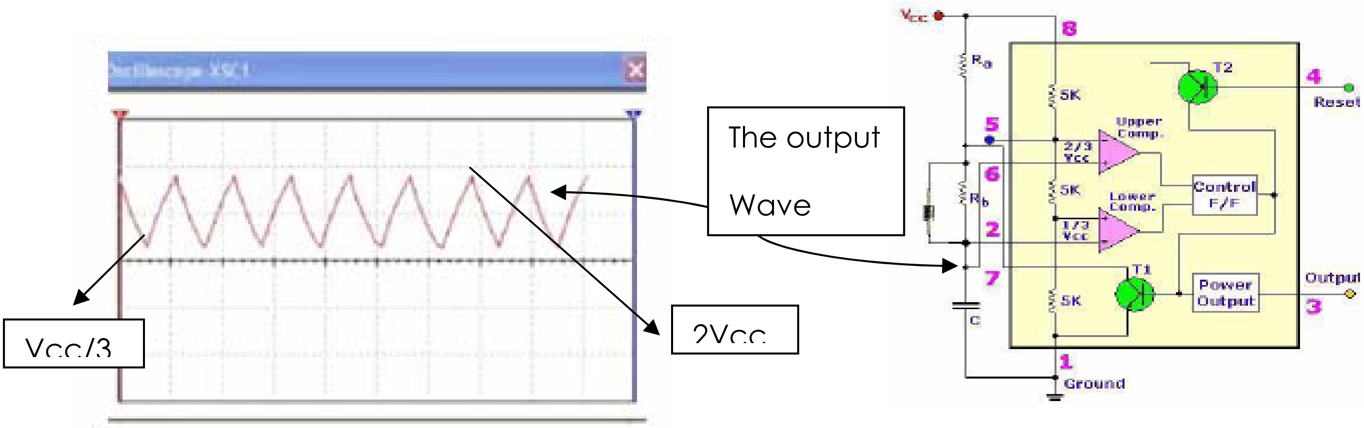


Figure 4 A-stable mode connection [D.C.=50%].

In our project, we used Ra=Rb=750 Ω with C=0.1 μF, then the output frequency is 10 KHz Since we use +12 V (Vcc), the output signal will be bounded from 4 V (Vcc/3) to 8 V (2Vcc/3). Figure 5 shows all the components used to generate the triangular wave. The output is shown in figure 6.

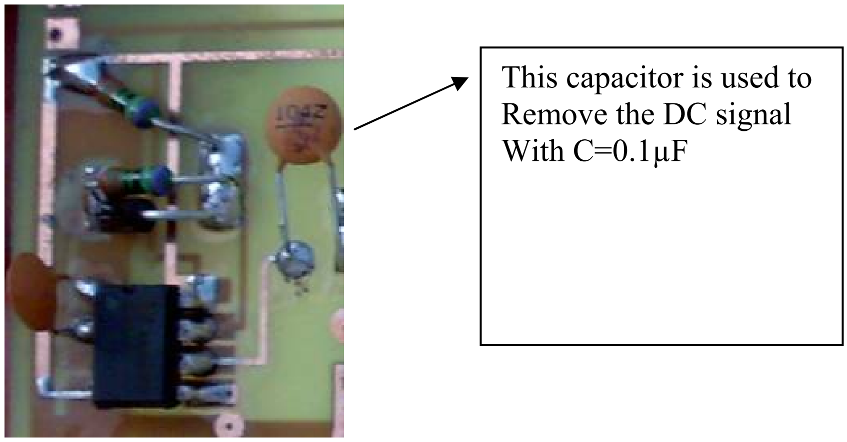


Figure 5 Triangular wave generator.

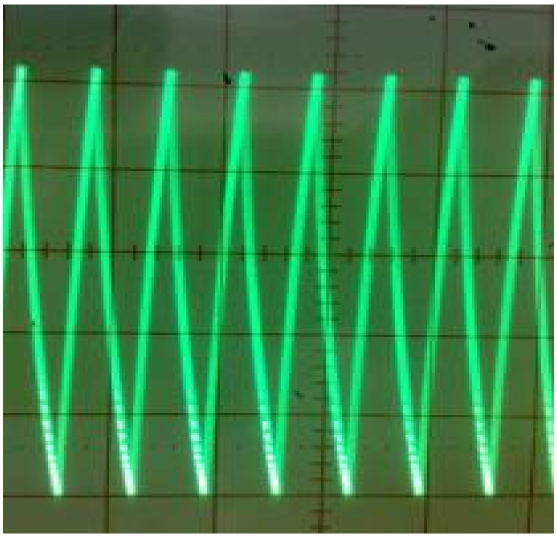


Figure 6 Generated triangular waveform.

Noise generation

Without noise, the output of the VCO is just an un-modulated sweeping RF carrier. So, we need to mix the triangular signal with noise (FM modulating the RF carrier with noise). To generate noise signal, we used the Zener Diode operated in reverse mode. Operating in the reverse mode causes what is called avalanche effect, which causes wide band noise. This noise is then amplified and used in our system. We use two amplification stages: in the first stage, we use NPN transistor as common emitter, and in the second stage, we use the LM386 IC {Audio amplifier}. This is shown in Figure 7. The output of this section is clearly seen in Figure 8.

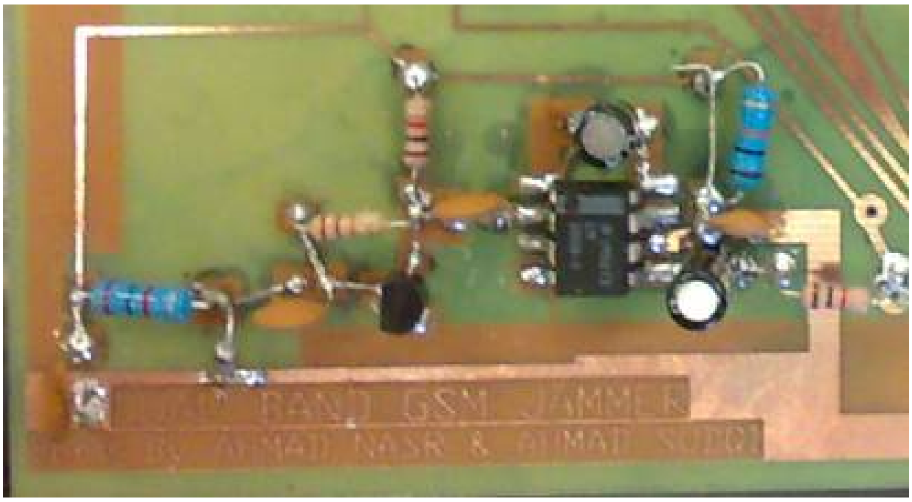


Figure 7 The noise generation.

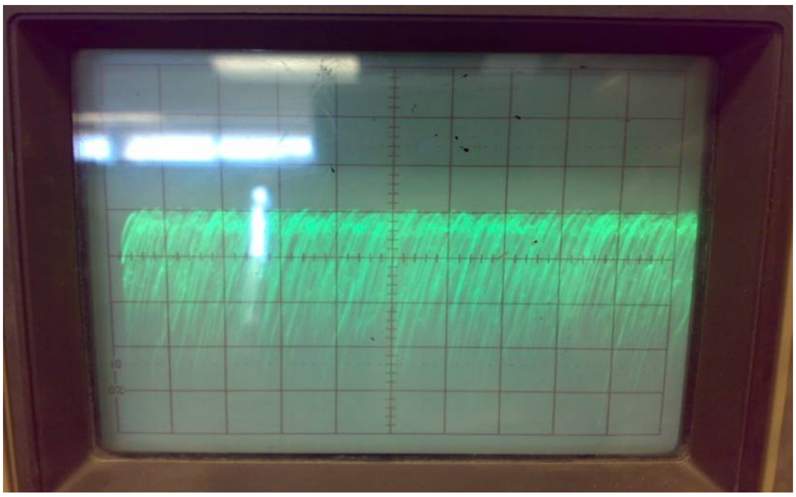


Figure 8 The generated noise signal.

Mixer

The mixer here is just an amplifier that operates as a summer. So, the noise and triangular wave will add together before entering the VCO. The LM741 IC was used to achieve this.

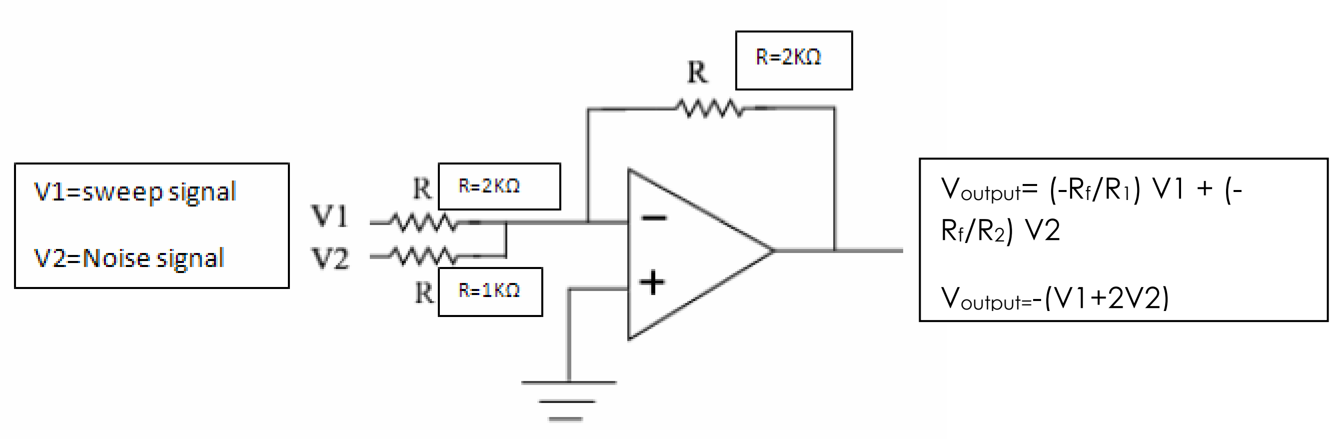


Figure 9 OP-AMP summer circuit

Using R_{noise} =1 KΩ, we amplify the noise signal by 2. In this case, the ratio of the noise to the sweep signal is 2:1.

Clamper

The input of the VCO must be bounded from 0 to 3.5 V to get the needed frequency range. So, we need to add a clamper to get our goal. The clamper consists of a capacitor connected in series with a resistor and diode, as shown in Figure 10.

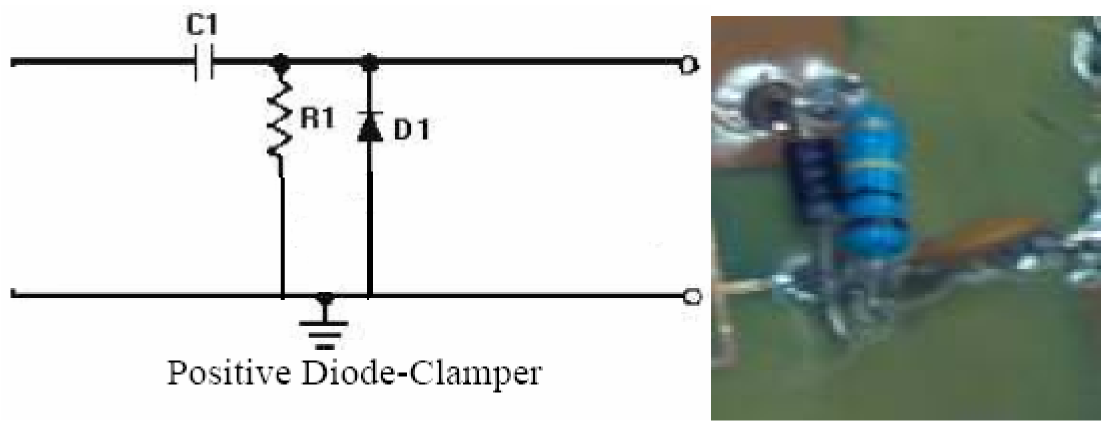


Figure 10 Diode clamper.

Then, the sweep signal that will sweep the RF-section is as shown in Figure 11. The tuning signal is highly noisy as seen in Figure 11. The whole IF-Section is seen in Figure 12. The IF-section schematic is shown in Figure 13.

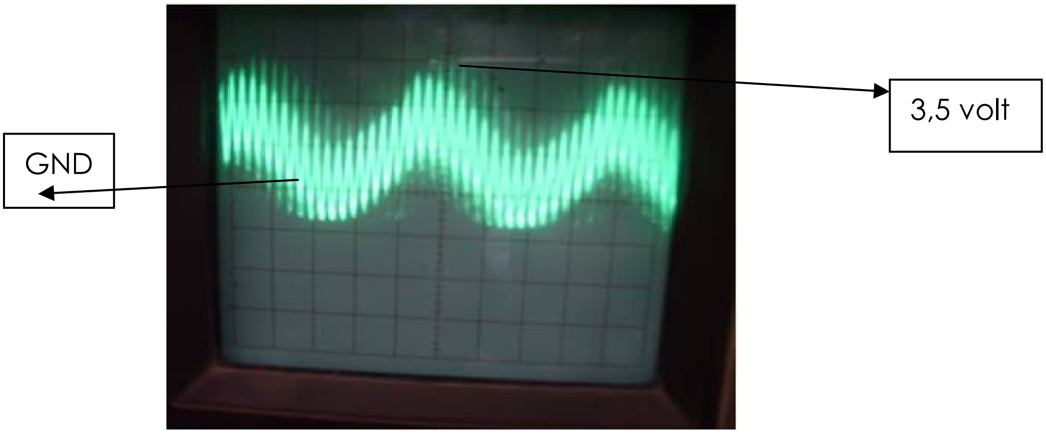


Figure 11 Tuning signal.

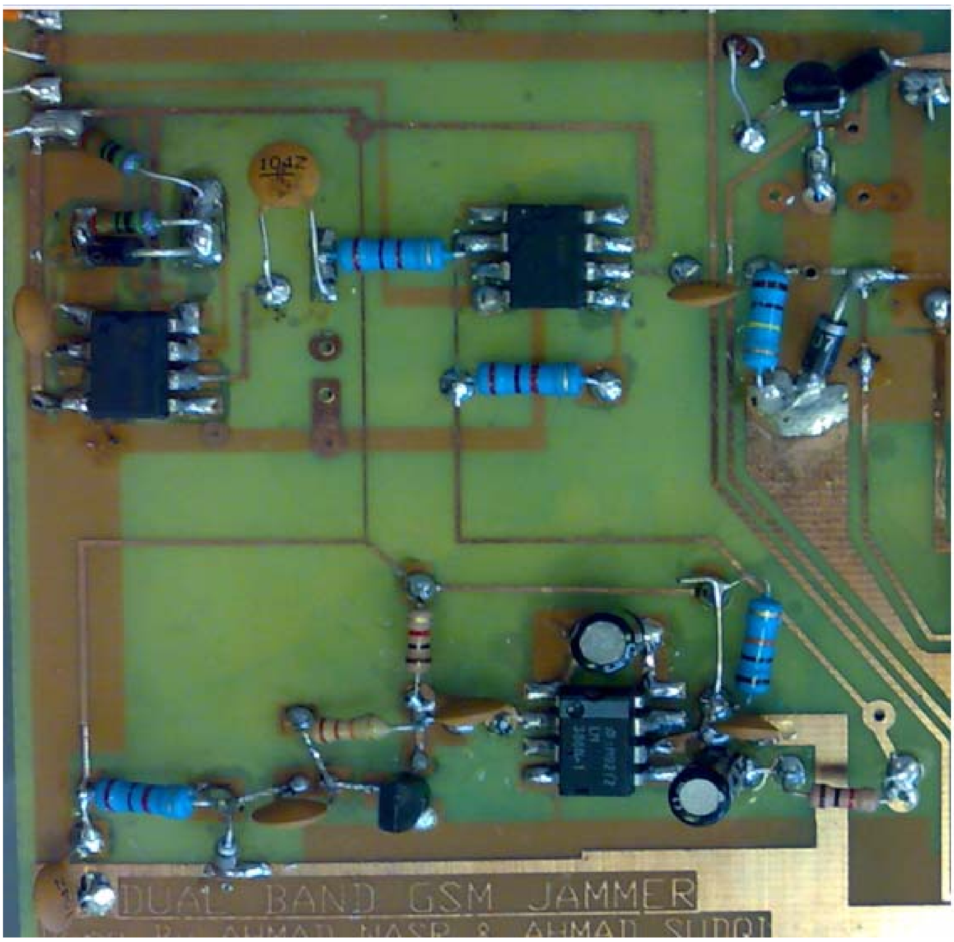


Figure 12 Picture of the designed IF-section.

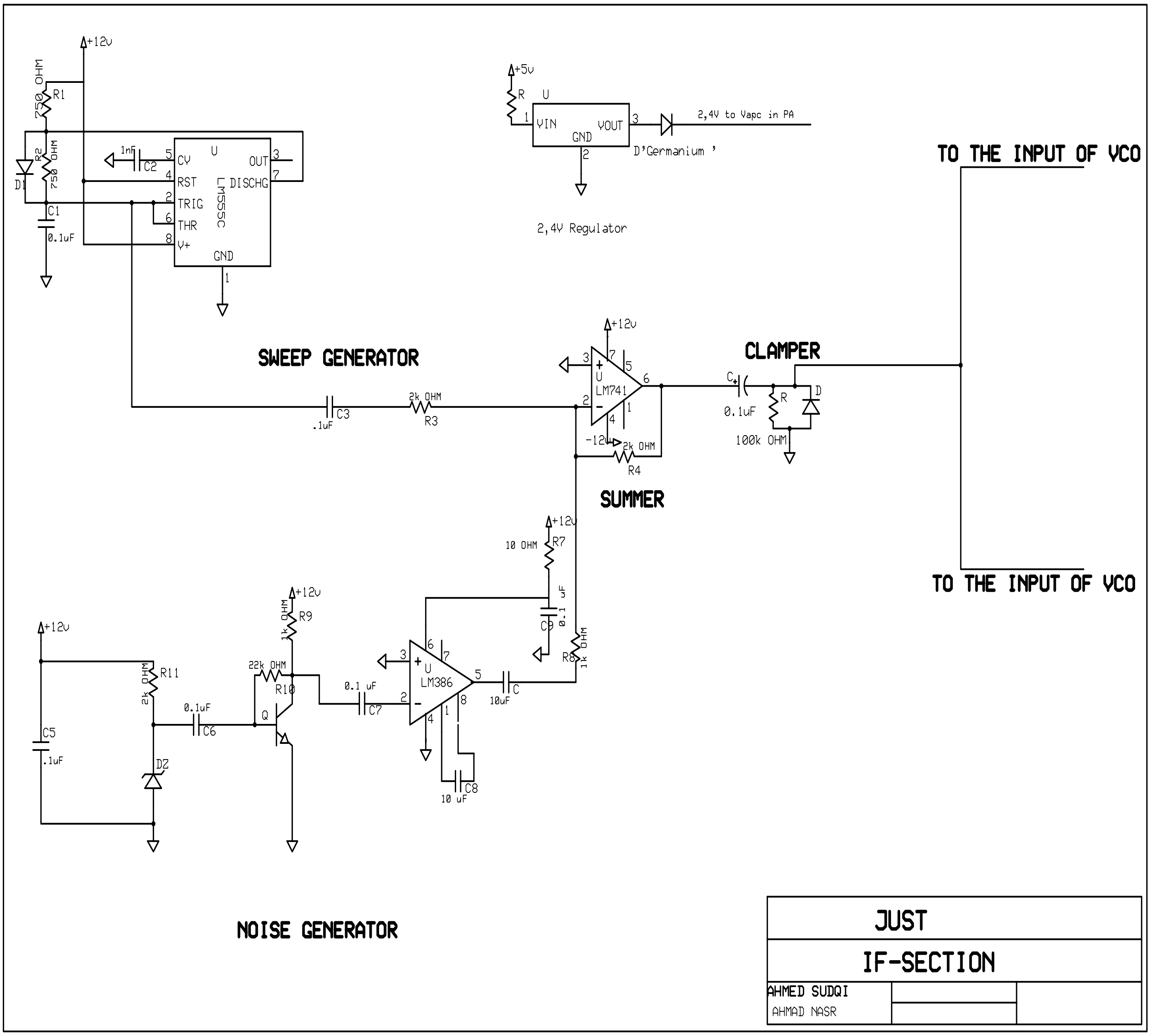


Figure 13 Schematic of the IF-section.

4.2.3 The RF-Section

This is the most important part of the jammer, since the output of this section will be interfacing with the mobile. The RF-section consists of three main parts: voltage controlled oscillator VCO, power amplifier and antenna.

The voltage controlled oscillator (VCO) is the heart of the RF-section. It is the device that generates the RF signal which will interfere with the cell phone. The output of the VCO has a frequency which is proportional to the input voltage, thus, we can control the output frequency by changing the input voltage. When the input voltage is DC, the output is a specific frequency, while if the input is a triangular waveform, the output will span a specific frequency range. In our design, we need to find a VCO for GSM 900 and GSM 1800. There are three selection criteria for selecting a VCO for this application. Most importantly, it should cover the bands that we need, secondly, it should be readily available at low cost, and finally, it should run at low power consumption. Moreover, we need to minimize the size of GSM-jammer. So, we started to search through the internet for VCO's that work for GSM 900 & GSM 1800 bands.

Finally, we found the following VCO IC's:-

CVCO55BE; this is for GSM 1800. The output frequency is 1785-1900 MHz and the output power is up to 5 dBm.

CVCO55CL; this is for GSM 900. The output frequency is 925-970 MHz and the output power is up to 8 dBm.

We chose these IC's for the following reasons:-

[A] Surface mount, which reduces the size of product.

[B] Having large output power that reduces the number of amplification stages that we need.

[C] Having same value of power supply which is typically equal to 5 volt.

[D] Having same noise properties.

Figure 14 shows these two IC's.

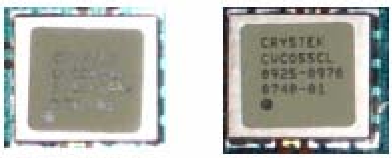


Figure 14 The VCO IC'S

The power amplifier: Since 5 dBm output power from the VCO does not achieve the desired output power of the GSM jammer, we had to add an amplifier with a suitable gain to increase the VCO output to 34 dBm. We obtained our amplifier IC (PF08109B) from an old mobile as it was the most suitable, cheapest and easiest way to get one.

The PF08109B, shown in Figure 15, has high gain of 35 dB. As datasheets illustrated that this IC is designed to work in dual band GSM & DCS, we firstly designed and built our circuit using only one power amplifier IC. Upon testing, the jammer didn't work properly. It was concluded that amplifier IC does not work at the two bands simultaneously. Such a fact was not indicated in the datasheets. This result was really a big shock, but easily solved by changing the whole RF design. The new design uses two power amplifier IC's instead of one amplifier. Figure 16 shows the two designs for the RF-Section.

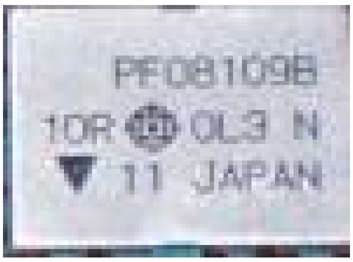


Figure 15 The power amplifier IC.

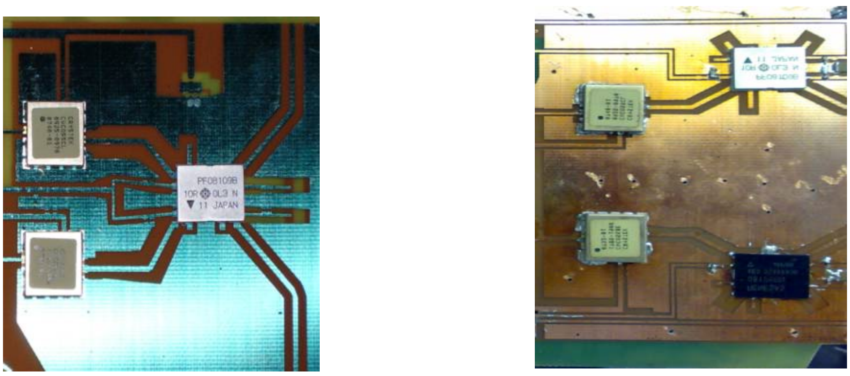


Figure 16 The RF-Section.

Antenna: A proper antenna is necessary to transmit the jamming signal. In order to have optimal power transfer, the antenna system must be matched to the transmission system. In this project, we used two 1/4 wavelength monopole antennas, with 50 Ω input impedance so that the antennas are matched to the system. We used monopole antenna since the radiation pattern is omni-directional. Figure 17 shows the DCS 1800 antenna, while Figure 18 shows the GSM 900 antenna.

Specifications:

- ✓ Frequency: 1700-1900MHz
- ✓ Input impedance 50Ω
- ✓ VSWR<2



Figure 17 The DCS Antenna.

Specifications:

- ✓ Frequency: 850MHz-1GHz
- ✓ Input impedance 50Ω
- ✓ VSWR<2



Figure 18 The GSM 900 antenna.

Figure 19 shows the RF-Section. The traces in the RF-section were designed to get 50 Ω impedance to insure matching between the IC's and the board.

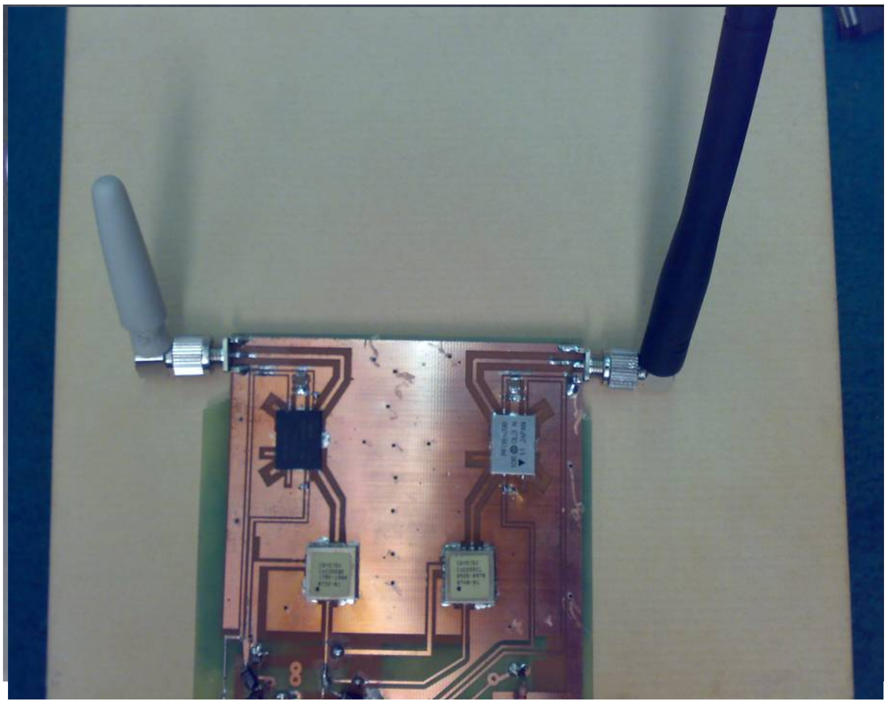


Figure 19 Picture of the RF-Section.

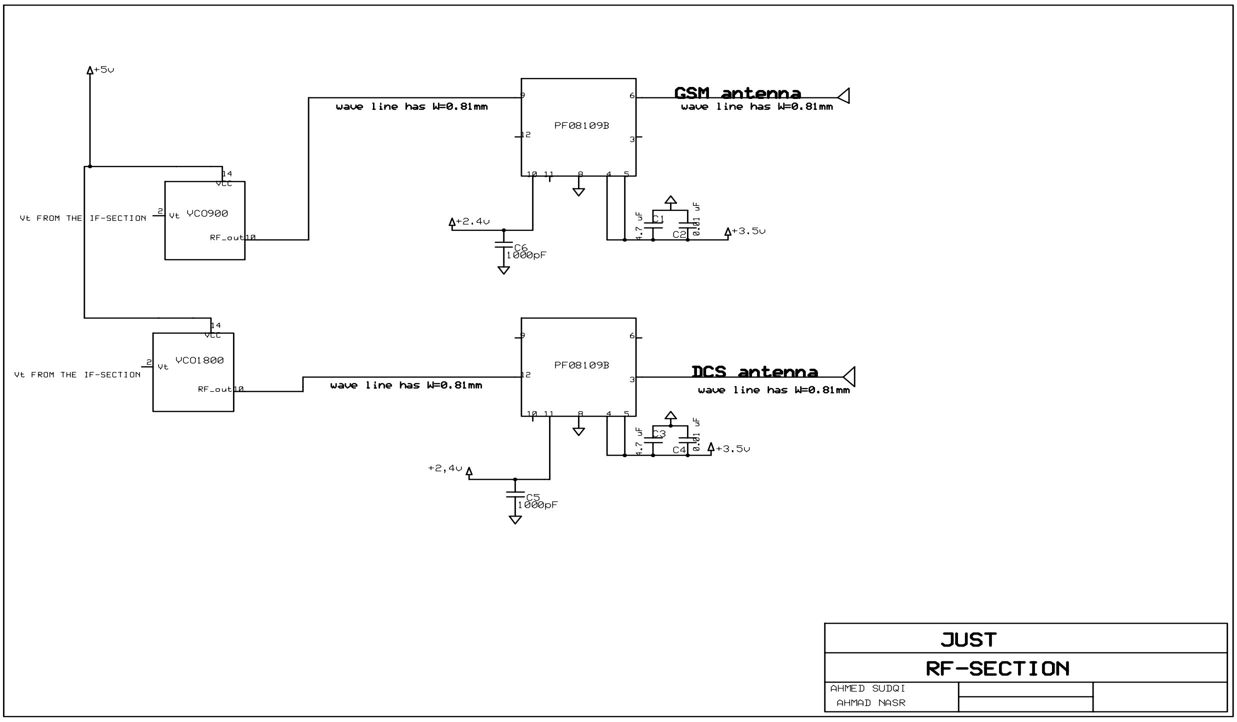


Figure 20 RF-section Schematic.

A picture of the whole jammer device is shown in Figure 21. The dimensions for the jammer are clearly seen in Figure 22. It is such a cute, small and portable device!

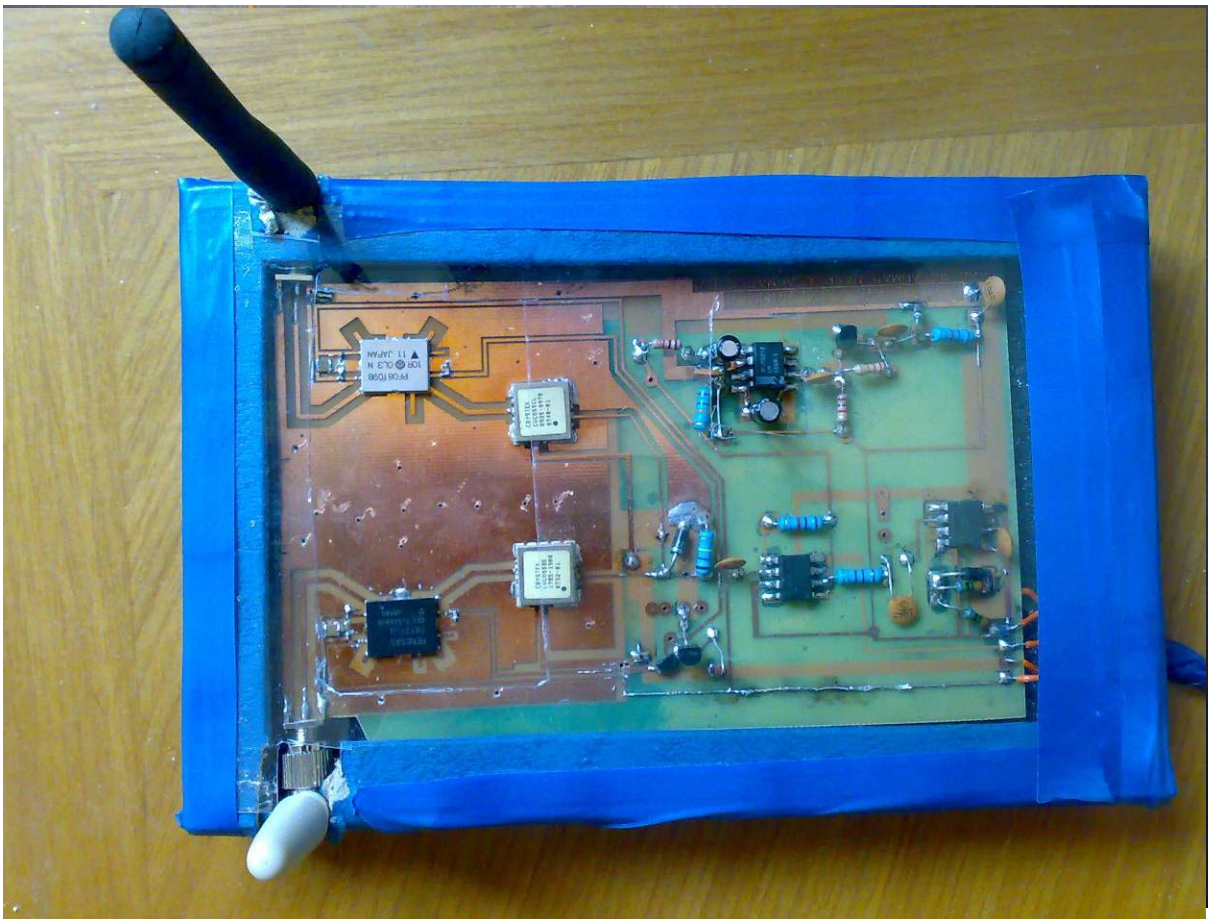


Figure 21 The jammer device.

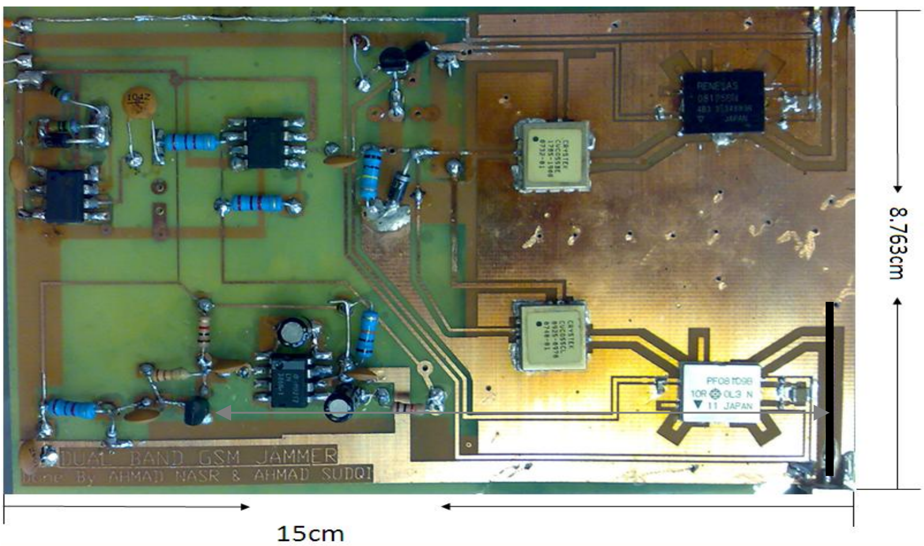


Figure 22 Dimensions of jammer.

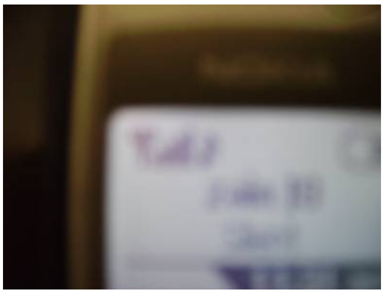
5. Results

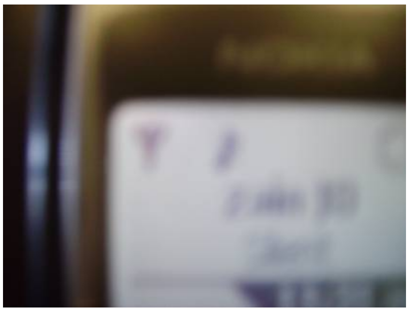
As we tested our jamming device, the result was a full success. The device was able to jam the three cell phone carriers: Zain, Orange, and Umniah. The effective jamming range was around 30 meters. This is more than what it was designed for. The reason is that in our calculations, we considered the worst case of having the cell phone close to the base station. It is expected that as the distance between the cell phone and the base station increases, the effective jamming distance will increase. This is due to the fact that the amount of power reaching the cell phone from the base station decreases as the cell phone moves farther from the base station. The Figure in the next page shows the results. It can be clearly seen that the signal is "ON" when the jammer is "OFF", while the signal disappears when the jammer is "ON".

[1] Zain

Jammer off

Jammer on





[2] Orange

Jammer off

jammer on





3] Umniah

Jammer off

jammer on





6. Conclusions

In this project, which turned out to be a full success, we designed a device that stops phone ringing. This device could be used in places where ringing is not desired at specific times, as these ringings may disturb people in such places. The designed device works in dual band. It jams both the GSM 900 and GSM 1800 bands. The device was able to jam the three main cell phone carriers in Jordan.

The project was implemented according to the following plan:

- We started by studying the jamming techniques, and GSM system to find the best jamming method. The system block diagram was also specified in this stage.
- We searched for components that are needed for building this device, and specified the main components which were :
  - For RF section, we needed two VCO's that operate at the needed bands, two power amplifier, and two antennas.
  - For the IF section, we used 555timer, Zener diode, mixer, PC power supply and some discrete components (resistors and capacitors).
- The schematic was drawn and some simulations for the IF-Section were performed. Then, we started to design the layout using Express PCB and AutoCAD softwares. The PCB was built using the etching process on copper clad board.
- All the IF-components were bought from local companies. Then, the IF-section was built and tested.
- After that, we began to search for the RF-components (VCO and the board) in the local market. Since we failed to collect these IC's from the local market, we had to order them from "Digi-key" US company.
- Finally, we assembled and tested the jammer. Fortunately, we got positive results. Both bands were fully jammed.

We hope that this project will be useful for the community where such jamming devices are needed.

References

1. Rick Hartley, RF / Microwave PC Board Design and Layout, Avionics Systems.
2. John Scourias, Overview of the Global System for Mobile Communications, University of Waterloo.
3. Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, JUST, 2006.
4. Limor Fried, Social Defense Mechanisms: Tools for Reclaiming our Personal Space.
5. Siwiak, K., Radio-wave propagation and Antennas for personal communication.
6. Pozar, D., Microwave Engineering, John Wiley and Sons, 2005.
7. "FREQUENCY PLANNING AND FREQUENCY COORDINATION FOR THE GSM 900, GSM 1800, E-GSM and GSM-R LAND MOBILE SYSTEMS (Except direct mode operation (DMO) channels)" by Working Group Frequency Management" (WGFM).
8. Tony Van Roon, 555 timer tutorial.

Appendix

Parts and Prices

	Part	amount	Total Price
Power supply	Power Supply 24bin	1	10 JD
IF section	Resistor	10	0.5 JD
	Capacitor	10	1.5 JD
	555 timer IC	1	0.5 JD
	LM741	1	0.5 JD
	LM386	1	1.25 JD
	Zener Diode 6.8 v	1	0.15 JD
	Diode	2	0.3 JD
RF section	PCB COPPER CLAD 6*9” 2-SIDE	1	21.36 USD
	OSC VCO 925-970MHz SMD .5X.5”	1	29.50 USD
	OSC VCO 1785-1900MHz SMD .5X.5”	1	28.75 USD
	PF08109B Power Amplifier	2	Old mobile phones

The layout of the jammer

- Dimensions are in mm.
- Drawing not to scale.

